

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-215027

(43)Date of publication of application : 31.07.2002

(51)Int.Cl.

G09C 1/00
H04L 9/32

(21)Application number : 2001-013529

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 22.01.2001

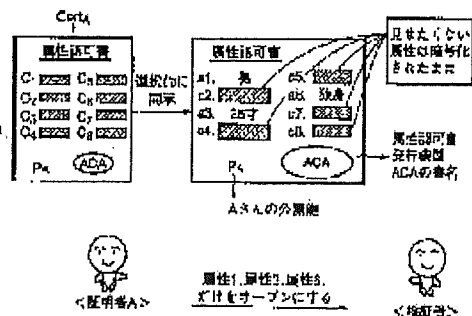
(72)Inventor : MIYAZAKI SHINGO
KAWAMURA SHINICHI

(54) ATTRIBUTE CERTIFICATION PROGRAM AND DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To realize certification and signature techniques which can be applied to various systems and contribute to development of an information-oriented society.

SOLUTION: The attribute certificate is provided which includes a lot of attribute information so that they can be individually verified. Concretely, (1) an attribute certificate CertA is a digital signature of an attribute certificate issue agency ACA which is given to a public key PA of a prover A, attribute information c1 to c8 ciphered by a key, and the total number 8 of attributes. (2) The prover A discloses attribute information a1, a3, and a6, which are related to only attributes of which the disclosure is requested, to a verifier and proves it to the verifier that disclosed attribute information a1, a3, and a6 are permitted right information. (3) Attribute information a2, a4, a5, a7, and a8 related to attributes of which the disclosure is not requested are not disclosed to the verifier at all. Thus various certificates/signatures using minimum required attributes are possible.



(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開2002-215027

(P2002-215027A)

(43)公開日 平成14年7月31日(2002.7.31)

(51)Int.Cl.⁷

G 0 9 C 1/00

識別記号

6 4 0

F I

G 0 9 C 1/00

テ-マコ-ト*(参考)

6 4 0 B 5 J 1 0 4

6 4 0 Z

H 0 4 L 9/32

H 0 4 L 9/00

6 7 5 B

6 7 5 D

審査請求 未請求 請求項の数14 O L (全 12 頁)

(21)出願番号 特願2001-13529(P2001-13529)

(22)出願日 平成13年1月22日(2001.1.22)

(71)出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72)発明者 宮崎 真悟

東京都府中市東芝町1番地 株式会社東芝
府中事業所内

(72)発明者 川村 信一

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(74)代理人 100058479

弁理士 鈴江 武彦 (外6名)

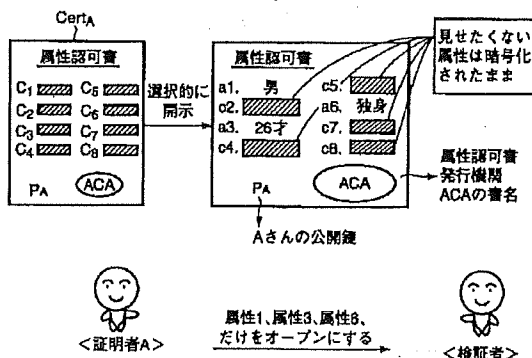
Fターム(参考) 5J104 AA07 KA01 KA05 LA05 MA02
NA02 NA12

(54)【発明の名称】 属性証明プログラム及び装置

(57)【要約】

【課題】 各種システムに適用でき、情報化社会の発展に寄与できる認証・署名技術を実現する。

【解決手段】 複数の属性情報を個別に検証可能に含めた属性認可書を設ける。具体的には(1)属性認可書Cert_Aは、証明者の公開鍵P_A、鍵暗号化された属性情報c₁~c₈、及び属性の総数8、に対して施された属性認可書発行機関ACAのデジタル署名とする。(2)証明者Aは、開示要求された属性のみに関する属性情報a₁, a₃, a₅を検証者に開示でき、また、開示された属性情報a₁, a₃, a₅が認可された正当な情報であることを検証者に証明できる。(3)開示要求されていない属性に関する属性情報a₂, a₄, a₆, a₇, a₈は検証者に一切露呈しない。よって必要最小限の属性を用いた各種証明/署名が可能である。



【特許請求の範囲】

【請求項 1】 n 個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内の n 個の属性情報のうち、n 個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される属性証明プログラムであって、前記利用者装置のコンピュータを、前記属性認可書の発行の際に、秘密鍵及び公開鍵を生成する鍵生成手段、入力された内容に基づいて前記 n 個の属性情報を生成し、当該 n 個の属性情報及び前記鍵生成手段により生成された公開鍵を前記属性認可書発行機関装置に提示する属性情報生成手段、前記属性認可書発行機関装置から受けた属性認可書を検証する属性認可書検証手段、として機能させ、前記検証者装置による検証の際に、前記属性認可書の検証用データと、チャレンジに基づいて計算した属性証明並びに前記 n 個以下の属性情報の検証用データとを同時に又は別々に前記検証者装置に送信する属性証明生成手段、として機能させるための属性証明プログラム。

【請求項 2】 請求項 1 に記載の属性証明プログラムにおいて、

前記属性証明生成手段は、前記チャレンジのハッシュ値を算出し、このハッシュ値に基づいて前記属性証明を算出することを特徴とする属性証明プログラム。

【請求項 3】 請求項 1 又は請求項 2 に記載の属性証明プログラムにおいて、

前記属性証明生成手段は、
「前記同時に又は別々に」に代えて「同時に」とし、且つ前記チャレンジを生成する処理を含むことを特徴とする属性証明プログラム。

【請求項 4】 n 個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内の n 個の属性情報のうち、n 個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される属性証明プログラムであって、前記属性認可書発行機関装置のコンピュータを、前記利用者装置から提示された各属性情報に関して正否かを審査する属性情報審査手段、前記属性情報審査手段による審査結果が正当である旨を示すとき、前記 n 個の属性情報を埋め込んで属性認可書を発行し、当該属性認可書を利用者装置に送信する属性認可書発行手段、として機能させるための属性証明プログラム。

【請求項 5】 n 個の属性情報の埋め込まれた属性認可

書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内の n 個の属性情報のうち、n 個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される属性証明プログラムであって、前記検証者装置のコンピュータを、前記利用者装置から受けた前記属性認可書の検証用データに基づいて、前記属性認可書の正当性を検証する属性認可書検証手段、

10 前記属性認可書検証手段による検証結果が正当性を示すとき、前記利用者装置から受けた属性証明及び前記 n 個以下の属性情報に関し、各々正当性を検証する属性証明検証手段、として機能させるための属性証明プログラム。

【請求項 6】 請求項 5 に記載の属性証明プログラムにおいて、

前記検証者装置のコンピュータを、前記属性認可書検証手段による検証結果が正当性を示すとき、n 個以下の属性を指定する属性情報生成手段、前記属性情報生成手段により属性が指定されると、チャレンジを生成し、当該チャレンジ及び前記指定内容を前記利用者装置に送信するチャレンジ生成手段、として機能させるための属性証明プログラム。

【請求項 7】 請求項 5 又は請求項 6 に記載の属性証明プログラムにおいて、

前記属性証明検証手段による検証結果が正当性を示すとき、前記開示された n 個以下の属性情報の内容に基づいて、所定の対象システムの実行を許可する対象実行許可手段、

30 として機能させるための属性証明プログラム。

【請求項 8】 n 個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内の n 個の属性情報のうち、n 個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される前記利用者装置であって、

前記属性認可書の発行の際に、秘密鍵及び公開鍵を生成する鍵生成手段と、

入力された内容に基づいて前記 n 個の属性情報を生成し、当該 n 個の属性情報及び前記鍵生成手段により生成された公開鍵を前記属性認可書発行機関装置に提示する属性情報生成手段と、

前記属性認可書発行機関装置から受けた属性認可書を検証する属性認可書検証手段と、

前記検証者装置による検証の際に、前記属性認可書の検証用データと、チャレンジに基づいて計算した属性証明並びに前記 n 個以下の属性情報の検証用データとを同時に又は別々に前記検証者装置に送信する属性証明生成手

50

段と、

を備えたことを特徴とする利用者装置。

【請求項9】 請求項8に記載の利用者装置において、前記属性証明生成手段は、前記チャレンジのハッシュ値を算出し、このハッシュ値に基づいて前記属性証明を算出することを特徴とする利用者装置。

【請求項10】 請求項8又は請求項9に記載の利用者装置において、前記属性証明生成手段は、

「前記同時に又は別々に」に代えて「同時に」とし、且つ前記チャレンジを生成する処理を含むことを特徴とする利用者装置。

【請求項11】 n 個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内の n 個の属性情報のうち、 n 個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される前記属性認可書発行機関装置であって、前記利用者装置から提示された各属性情報に関して正

当か否かを審査する属性情報審査手段と、前記属性情報審査手段による審査結果が正当である旨を示すとき、前記 n 個の属性情報を埋め込んで属性認可書を発行し、当該属性認可書を利用者装置に送信する属性認可書発行手段と、

を備えたことを特徴とする属性認可書発行機関装置。

【請求項12】 n 個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内の n 個の属性情報のうち、 n 個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される前記検証者装置であって、前記利用者装置から受けた前記属性認可書の検証用データに基づいて、前記属性認可書の正当性を検証する属性認可書検証手段と、

前記属性認可書検証手段による検証結果が正当性を示すとき、前記利用者装置から受けた属性証明及び前記 n 個以下の属性情報に関し、各々正当性を検証する属性証明検証手段と、

を備えたことを特徴とする検証者装置。

【請求項13】 請求項12に記載の検証者装置において、

前記属性認可書検証手段による検証結果が正当性を示すとき、 n 個以下の属性を指定する属性情報生成手段と、前記属性情報生成手段により属性が指定されると、チャレンジを生成し、当該チャレンジ及び前記指定内容を前記利用者装置に送信するチャレンジ生成手段と、

を備えたことを特徴とする検証者装置。

【請求項14】 請求項12又は請求項13に記載の検

証者装置において、

前記属性証明検証手段による検証結果が正当性を示すとき、前記開示された n 個以下の属性情報の内容に基づいて、所定の対象システムの実行を許可する対象実行許可手段を備えたことを特徴とする検証者装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、各種システムに応用可能な属性証明プログラム及び装置に関する。

【0002】

【従来の技術】近年の情報化社会では、各端末装置間でのデータ通信の際に、データの正当性を認証するデジタル署名及びメッセージ認証や、通信相手の正当性を認証する相手認証といった認証・署名技術が広く用いられている。

【0003】係る認証・署名技術は、例えば証明者（署名者）が自己の秘密鍵情報により認証や署名を行なう方式となっている。また、検証者は、証明者（署名者）の公開鍵情報により、例えば証明者の署名を検証すればよい。

【0004】

【発明が解決しようとする課題】以上のような認証・署名技術は、情報化社会を支える暗号技術の中でも必要性の高いものであり、情報化社会を進展させる観点から、各種の応用手法が開発されることが好ましい。

【0005】本発明は上記実情を考慮してなされたもので、各種システムに応用でき、情報化社会の発展に寄与し得る属性証明プログラム及び装置を提供することを目的とする。

【0006】

【課題を解決するための手段】本発明の骨子は、複数の属性情報を個別に検証可能に含めた属性認可書を設ける構成により、各種システムに応用し得る認証・署名技術を提供することにある。

【0007】係る本発明は以下の（1）～（3）に示す性質を有する。

【0008】（1）属性認可書 Cert_A は、図6の例で述べると、証明者の公開鍵 P_A、鍵号化された属性情報 c₁～c_s、及び属性の総数 $n (= 8)$ 、に対して施された属性認可書発行機関 ACA のデジタル署名である。

【0009】（2）証明者 A は、開示要求された属性のみに関する属性情報 a₁, a₃, a₈ を検証者に開示でき、また、開示された属性情報 a₁, a₃, a₈ が認可された正当な情報である旨を検証者に証明することができる。

【0010】（3）開示要求されていない属性に関する属性情報 a₂, a₄, a₅, a₇, a₈ は検証者に一切露ししない。よって必要最小限の属性を用いた各種証明／署名が可能である。

【0011】係る本発明は、図7（a）に示す従来の秘密鍵による署名に比べ、図7（b）に示すように各属性

1～3を含む署名である点で異なり、さらに、図6に示したように、各属性を選択的に開示できる点で優れている。

【0012】さて、以上のような本発明の骨子について具体的には以下のような手段が講じられる。なお、各発明は、記載の簡潔性の観点から、プログラムとして表現された場合のみを示すが、装置、方法、システム等の他のカテゴリーで表現してもよいことは言うまでもない。各発明の適用対象は、 n 個の属性情報の埋め込まれた属性認可書を利用する利用者装置、前記利用者装置に前記属性認可書を発行する属性認可書発行機関装置、及び前記利用者装置から受けた前記属性認可書を検証し且つ前記属性認可書内の n 個の属性情報のうち、 n 個以下の属性情報を検証する検証者装置を備えた属性証明システムに使用される属性証明プログラムである。

【0013】第1の発明は、前記利用者装置のコンピュータを、前記属性認可書の発行の際に、秘密鍵及び公開鍵を生成する鍵生成手段、入力された内容に基づいて前記 n 個の属性情報を生成し、当該 n 個の属性情報及び前記鍵生成手段により生成された公開鍵を前記属性認可書発行機関装置に提示する属性情報生成手段、前記属性認可書発行機関装置から受けた属性認可書を検証する属性認可書検証手段、として機能させ、前記検証者装置による検証の際に、前記属性認可書の検証用データと、チャレンジに基づいて計算した属性証明並びに前記 n 個以下の属性情報の検証用データとを同時に又は別々に前記検証者装置に送信する属性証明生成手段、として機能させるための属性証明プログラムである。

【0014】ここで、前記属性証明生成手段は、セキュリティ性向上の観点から、前記チャレンジのハッシュ値を算出し、このハッシュ値に基づいて前記属性証明を算出してよい。

【0015】また、前記属性証明生成手段は、利用者（証明者）が自分でチャレンジを生成する属性署名（属性付き署名）に適用する場合の観点から、「前記同時に又は別々に」に代えて「同時に」とし、且つ前記チャレンジを生成する処理を含めてもよい。

【0016】第2の発明は、前記属性認可書発行機関装置のコンピュータを、前記利用者装置から提示された各属性情報に関して正当か否かを審査する属性情報審査手段、前記属性情報審査手段による審査結果が正当である旨を示すとき、前記 n 個の属性情報を埋め込んで属性認可書を発行し、当該属性認可書を利用者装置に送信する属性認可書発行手段、として機能させるための属性証明プログラムである。

【0017】第3の発明は、前記検証者装置のコンピュータを、前記利用者装置から受けた前記属性認可書の検証用データに基づいて、前記属性認可書の正当性を検証する属性認可書検証手段、前記属性認可書検証手段による検証結果が正当性を示すとき、前記利用者装置から受

けた属性証明及び前記 n 個以下の属性情報に関し、各々正当性を検証する属性証明検証手段、として機能させるための属性証明プログラムである。

【0018】ここで、第3の発明は、検証者が自分でチャレンジを生成する場合に適用する観点から、前記属性認可書検証手段による検証結果が正当性を示すとき、 n 個以下の属性を指定する属性情報生成手段、前記属性情報生成手段により属性が指定されると、チャレンジを生成し、当該チャレンジ及び前記指定内容を前記利用者装置に送信するチャレンジ生成手段、として機能させるための属性証明プログラムであってもよい。

【0019】なお、第3の発明は、さらに、前記属性証明検証手段による検証結果が正当性を示すとき、前記開示された n 個以下の属性情報の内容に基づいて、所定の対象システムの実行を許可する対象実行許可手段、として機能させるための属性証明プログラムとしてもよい。

【0020】（作用）従って、本発明は以上のような手段を講じたことにより、 n 個の属性情報の埋め込まれた属性認可書を利用し、開示要求される n 個以下の属性情報のみを検証者に開示し、開示要求されない属性情報を隠蔽できる。

【0021】このように、各種証明／署名の際に、属性情報を選択的に開示する属性証明システムを構築できるので、各種システムに応用でき、情報化社会の発展に寄与することができる。

【0022】

【発明の実施の形態】以下、本発明の各実施形態について図面を参照して説明する。なお、各実施形態で 사용되는各種パラメータと記号は以下の通りである。

p, q : 十分に大きな素数で $p = 2q + 1$ の関係式を満たす。

g : 乗法群 Z_{p^*} での位数が q となるような生成器。（ g は、システム共通の値（第4を除く第1～第6実施形態）としてもよく、利用者装置Aが生成する値（第4～第6実施形態）としてもよい）

P_A : 利用者装置Aの公開鍵。

S_A : 利用者装置Aの秘密鍵。

Λ_0 : 属性認可書発行時に提示された属性群 $\{a_1, a_2, \dots, a_n\}$ 。

a_i : Λ_0 の i 番目 ($1 \leq i \leq n$) の属性情報 (attribute)

n : 属性情報の総数

r_i : i 番目 ($1 \leq i \leq n$) の乱数。

b_i : a_i のブラインド値 (blinded attribute)

c_i : b_i のコミット値 (committed blinded attribute)

h : 無衝突一方向性ハッシュ関数。

$\text{Sig}_{c_A}[D]$: データDに対する属性認可書発行機関の署名。

$\text{Veri}_{c_A}[D]$: データDに対する属性認可書発行機関の署名検証。

u : 属性証明時に利用者(証明者)装置Aが生成する乱数 ($\in {}_s\mathbb{Z}_{q^*}$)

v : 属性証明時に利用者(証明者)装置Aが計算する u のコミット値 ($v = g^u \pmod{p}$)

Λ : 属性証明時に開示要求のあった属性群。

m : 属性証明時に検証者装置Vが生成するチャレンジ ($\in \mathbb{Z}_{q^*}$) あるいは利用者

装置Aが生成する(このチャレンジの)ハッシュ値

$f(m)$: m を用いた Λ の属性証明

$x || y$: ビット列 x とビット列 y との結合。

【0023】(第1の実施形態)図1は本発明の第1の実施形態に係る属性証明システムの構成を示す模式図である。この属性証明システムは、利用者装置A、属性認可書発行機関装置ACA及び検証者装置Vを備えており、各装置A、ACA、Vは、それぞれハードウェア、ソフトウェア又はそれらの組合せにより構成可能となっている。なお、ソフトウェアにより構成される場合、各装置A、ACA、Vの機能を実現するためのプログラムが各装置A、ACA、Vのコンピュータに予めインストールされている。

【0024】利用者装置Aは、鍵生成部11、属性情報生成部12、属性認可書検証部13、属性情報管理部14及び属性証明生成部15を備えている。

【0025】鍵生成部11は、属性認可書 $Cert_A$ の発行前に、秘密鍵 S_A 及び公開鍵 P_A を生成し、属性認可書 $Cert_A$ の発行時に、これら秘密鍵 S_A 及び公開鍵 P_A を属性情報生成部12に送出する機能をもっている。

【0026】属性情報生成部12は、鍵生成部11から受けた秘密鍵 S_A を属性認可書検証部13に設定する機能と、利用者の入力操作により、承認して欲しい属性情報 $\{a_1, a_2, \dots, a_n\}$ を生成して属性情報管理部14に設定する機能と、公開鍵 P_A と承認して欲しい属性情報からなる属性群 $\Lambda = \{a_1, a_2, \dots, a_n\}$ とを属性認可書発行機関ACAに提示する機能をもっている。なお、属性情報は、何らかの部分情報であればよく、その内容は任意である。

【0027】属性認可書検証部13は、属性認可書発行機関ACAから受けた属性認可書 $Cert_A$ 及び n 個の乱数 (r_1, \dots, r_n) に基づいて、属性情報管理部14を参照しながら所定の検証処理(後述するST9)を行なう機能と、検証処理の終了後、属性認可書 $Cert_A$ 及び n 個の乱数 (r_1, \dots, r_n) を属性情報管理部14に保存する機能をもっている。

【0028】なお、属性認可書 $Cert_A$ は、属性認可書発行機関装置ACAによるデジタル署名 $Sig_{ACA}[h(P_A || n || c_1 || \dots || c_n)]$ である。

【0029】属性情報管理部14は、利用者装置A内の各情報を読み出/書込可能に保持・管理するものであり、具体的には、公開鍵 P_A 、秘密鍵 S_A 、各属性 $a_1 \sim a_n$ 、各乱数 $r_1 \sim r_n$ 、各コミット値 $c_1 \sim c_n$ 及び属性認可書

$Cert_A$ が管理可能となっている。なお、秘密鍵 S_A は、他の耐タンパー性メモリ(図示せず)で管理してもよい。

【0030】属性証明生成部15は、属性証明の際に、乱数 u 及びそのコミット値 v を生成する機能と、属性情報管理部14を参照して検証用データ $(v, Cert_A, n, P_A, c_1, \dots, c_n)$ を検証者装置Vに送信する機能と、検証者装置Vからチャレンジ m 及び属性群 Λ を受けると、要求された属性の開示を容認する場合、属性証明 $f(m)$ を計算する機能と、この属性証明 $f(m)$ 及びデータ (j, a_1, r_1) を検証者装置Vに送信する機能とをもっている。

【0031】また、利用者装置Aの実現形態としては、任意の形態が適用可能である。例えば、パーソナルコンピュータの如き設置型や可搬型、又は携帯電話や電子手帳の如き携帯型、あるいはそれらの組合せ(例、設置型の装置と、携帯型のICカードとの組合せ等)のいずれでもよく、その通信方式も有線又は無線のいずれでもよい。

【0032】属性認可書発行機関装置ACAは、属性情報審査部21及び属性認可書発行部22を備えている。

【0033】属性情報審査部21は、利用者装置Aから提示された属性群 Λ 内の各属性 a_i を利用者の情報として正当か否かを審査する機能と、審査結果を属性認可書発行部22に送出する機能とをもっている。

【0034】属性認可書発行部22は、属性情報審査部21から受けた審査結果が正当である旨を示すとき、所定の属性認可書発行処理(後述するST5~ST8)を実行する機能と、属性認可書発行処理の終了後、属性認可書 $Cert_A$ 、 n 個の乱数 (r_1, \dots, r_n) を利用者装置Aに送信する機能とをもっている。

【0035】検証者装置Vは、属性認可書検証部31、属性情報要求部32、チャレンジ生成部33及び属性証明検証部34を備えている。

【0036】属性認可書検証部31は、利用者装置Aから受けた検証用データ $(v, Cert_A, n, P_A, c_1, \dots, c_n)$ に基づいて、属性認可書 $Cert_A$ の正当性を検証する機能と、検証結果を属性情報要求部32に送出する機能とをもっている。

【0037】属性情報要求部32は、属性認可書検証部31から受けた検証結果が正当を示すとき、開示して欲しい属性(要求属性)からなる属性群 Λ をチャレンジ生成部33に送出する機能をもっている。

【0038】チャレンジ生成部33は、属性情報要求部32から属性群 Λ を受けると、チャレンジ m を生成する機能と、このチャレンジ m 及び属性群 Λ を属性証明検証部34及び利用者装置Aに送信する機能とをもっている。

【0039】属性証明検証部34は、利用者装置Aから受けた属性証明 $f(m)$ の正当性を検証する機能と、この

検証結果が正当を示すとき、開示された属性 a_i の正当性を検証する機能とをもっている。

【0040】次に、以上のように構成された属性証明システムの動作を図2及び図3のフローチャートを用いて、初期手続時の属性認可書発行、及び通常使用時の属性証明の順に説明する。

【0041】（属性認可書発行）図2に示すように、利用者装置Aにおいては、鍵生成部11が秘密鍵 $S_A \in_r Z_q$ を生成し（ST1）、公開鍵 $P_A = g^{S_A} \pmod{p}$ を計算すると（ST2）、これら秘密鍵 S_A 及び公開鍵 P_A を属性情報生成部12に送出する。

【0042】属性情報生成部12は、秘密鍵 S_A を属性認可書検証部13に設定し、承認して欲しい属性情報を生成して（ST3）属性情報管理部14に設定する一方、公開鍵 P_A と、承認して欲しい属性情報からなる属性群 Λ を属性認可書発行機関ACAに提示する。属性認可書発行機関ACAにおいては、属性情報審査部21が、提示された各属性 a_i を利用者の情報として正当か否かを審査し（ST4）、審査結果を属性認可書発行部22に送出する。

【0043】属性認可書発行部22は、審査結果が正当である旨を示すとき、以下の属性認可書発行処理（ST5～ST8）を実行する。

【0044】始めに、 n 個の乱数 $r_i \in_r Z_q^*$ を生成する（ST5）。

【0045】続いて、乱数 r_i と属性 a_i とを結合（連接）してハッシュ関数により、 n 個のブラインド値 $b_i = h(a_i || r_i)$ を計算する（ST6）。

【0046】次に、生成器 g に対し、各ブラインド値 b_i を用いて n 個のコミット値 $c_i = g^{b_i} \pmod{p}$ を計算する（ST7）。

【0047】最後に、公開鍵 P_A 、属性 a_i の総数 n 及び各コミット値 $c_1 \sim c_n$ を結合し、それらにハッシュ関数を介して得たハッシュ値に対し、自己の秘密鍵で署名を施すことにより、属性認可書 $Cert_A$ を発行する（ST8）。

【0048】 $Cert_A = \text{Sig}_{K_A} [h(P_A || n || c_1 || \dots || c_n)]$
このような属性認可書発行処理の終了後、属性認可書発行機関ACAは、属性認可書 $Cert_A$ 、 n 個の乱数 (r_1, \dots, r_n) を利用者装置Aに送信する。

【0049】一方、利用者装置Aでは、属性認可書検証部13が以下の検証処理を行う（ST9）。

【0050】始めに、属性情報管理部14から n 個の属性 $a_1 \sim a_n$ を得ると、これら各属性 a_i と各乱数 r_i とを結合してハッシュ関数により、 n 個のブラインド値 $b_i = h(a_i || r_i)$ を計算する。

【0051】次に、生成器 g に対し、各ブラインド値 b_i を用いて、 $c_i = g^{b_i} \pmod{p}$ を計算する。

【0052】最後に、公開鍵 P_A 、属性 a_i の総数 n 及び

各コミット値 $c_1 \sim c_n$ を結合し、それらにハッシュ関数を介して得たハッシュ値と、属性認可書 $Cert_A$ を属性認可書発行機関ACAの公開鍵で復号した復号結果とを比較することにより、属性認可書 $Cert_A$ の署名を検証する。

【0053】 $\text{Veri}_{K_A} [h(P_A || n || c_1 || \dots || c_n), Cert_A] = \text{valid}$ （正当）？

このような検証処理の終了後、検証結果が正当であれば、利用者装置Aは、属性認可書 $Cert_A$ 、各乱数 $r_1 \sim r_n$ 及び各コミット値 $c_1 \sim c_n$ を属性情報管理部14に保存する。

【0054】（属性証明）図3に示すように、利用者装置Aでは、属性証明生成部15が、乱数 $u \in_r Z_q^*$ を生成し、そのコミット値 $v = g^u \pmod{p}$ を計算する（ST11）。

【0055】しかる後、属性証明生成部15は、属性情報管理部14を参照して、乱数 u のコミット値 v 、属性認可書 $Cert_A$ 、属性 $a_1 \sim a_n$ の総数 n 、公開鍵 P_A 、属性 $a_1 \sim a_n$ のコミット値 c_1, \dots, c_n からなる検証用データ $(v, Cert_A, n, P_A, c_1, \dots, c_n)$ を検証者装置Vに送信する。

【0056】検証者装置Vは、属性認可書 $Cert_A$ の検証用データ $(v, Cert_A, n, P_A, c_1, \dots, c_n)$ を受けると、属性認可書検証部31により、属性認可書 $Cert_A$ の正当性を検証する（ST12）。

【0057】 $\text{Veri}_{K_A} [h(P_A || n || c_1 || \dots || c_n), Cert_A] = \text{valid}$ ？

これにより、検証者装置Aは、属性認可書 $Cert_A$ 内の全ての属性情報 $a_1 \sim a_n$ が認可された正当な情報である旨を検証する。正当性の検証処理の終了後、属性認可書検証部31は、検証結果を属性情報要求部32に送出する。

【0058】属性情報要求部32は、検証結果が正当であれば、開示して欲しい属性（要求属性）からなる属性群 Λ をチャレンジ生成部33に送出する。

【0059】チャレンジ生成部33は、チャレンジ $m \in_r Z_q^*$ を生成し（ST13）、チャレンジ m と、開示して欲しい属性からなる属性群 Λ とを自己の属性証明検証部34及び利用者装置Aに送信する。

【0060】利用者装置Aでは、チャレンジ m 及び属性群 Λ を受けると、属性証明生成部15が、開示要求された属性に対し、開示を容認する場合、最大で $n+1$ 次の多項式からなる属性証明 $f(m)$ を計算する（ST14）。

$f(m) = v S_A + u m + b_1 m^2 + \dots + b_n m^{n+1} \pmod{q}$

すなわち、属性証明 $f(m)$ は、開示要求された属性の総数が i 個の場合、次式のように $i+1$ 次となる。

$f(m) = v S_A + u m + b_1 m^2 + \dots + b_i m^{i+1} \pmod{q}$

なお、同式中の“ $b_1 \sim b_i$ ”の記載は、1番目～ i 番目の値に限定される趣旨とは異なり、開示要求に対応した i 個の“ b_i ”が用いられる趣旨であることは言うまでもない。これは後述する $f(m)$ の検証式中の“ c_i ”でも同様である。また、変形例として、開示、非開示に関わらず、 n 個全ての属性($b_1 \sim b_n$)で属性証明 $f(m)$ を生成する構成としてもよい。

【0061】いずれにしても、その後、属性証明生成部15は、属性証明 $f(m)$ と、開示要求のあった属性群 Λ に該当する属性番号 j 、属性 a_i 及び乱数 r_i からなる開示要求された属性情報の検証用データ(j, a_i, r_i)とを

検証者装置Vに送信する($j \in \Lambda$)。
【0062】検証者装置Vでは、属性証明検証部34が、この属性証明 $f(m)$ の正当性を次の第1検証式により検証する(ST15)。

【数1】

$$g^{f(m)} \equiv P_A^v v^m \prod_{i=1}^l c_i^{m^{i+1}} \pmod{p}$$

【0063】これにより、検証者装置Vは、属性認可書 $Cert_A$ 内の全ての属性情報 $a_1 \sim a_n$ のうち、開示要求された i 個の属性情報 $a_1 \sim a_i$ の全てが認可された正当な情報であることを検証することができる。また、検証結果が正当を示すとき、属性証明検証部34は、開示要求した属性 $j \in \Lambda$ について、ステップST12で受けたコミット値 c_j を使い、開示された属性 a_i の正当性を次の第2検証式のように個別に検証する(ST16)。

【数2】

$$c_j \equiv g^{h(a_j || r_j)} \pmod{p}$$

【0064】これにより、検証者装置Vは、属性認可書 $Cert_A$ 内の n 個の属性 $a_1 \sim a_n$ のうち、開示された属性 a_i のみを個別に検証することができる。

【0065】上述したように本実施形態によれば、 n 個の属性情報 $a_1 \sim a_n$ の埋め込まれた属性認可書 $Cert_A$ を利用し、開示要求された n 個以下の属性情報 a_i のみを検証者装置Vに開示し、開示要求されない属性情報を隠蔽できる。

【0066】このように、各種証明／署名の際に、属性情報 a_i を選択的に開示する属性証明システムを構築できるので、各種システムに応用でき、情報化社会の発展に寄与することができる。

【0067】すなわち、利用者装置Aは、ステップST12により、属性認可書 $Cert_A$ 内の全ての属性情報 $a_1 \sim a_n$ が認可された正当な情報であることを検証者装置Vに証明することができる。

【0068】また、利用者装置Aは、ステップST15により、属性認可書 $Cert_A$ 内の全ての属性情報 $a_1 \sim a_n$ のうち、開示要求された i 個の属性情報 $a_1 \sim a_i$ の全てが認可された正当な情報であることを検証者装置Vに証

明することができる。

【0069】さらに、利用者装置Aは、ステップST16により、各属性 a_i を個別に証明できるので、必要最小限の属性 a_i しか開示しなくとも済む。このため、開示要求されなかった属性情報を検証者から隠蔽・保護することができる。例えば、属性情報がプライバシーに関する内容である場合、開示要求されなかった属性情報に関するプライバシーを保護することができる。

【0070】(第2の実施形態)次に、本発明の第2の実施形態に係る属性証明システムについて述べるが、第1の実施形態と同一部分についてはその詳しい説明を省略し、ここでは異なる部分について主に述べる。なお、以下の各実施形態についても同様にして重複した説明を省略する。すなわち、本実施形態は、第1の実施形態の変形例であり、セキュリティの向上を図るものであって、具体的には、属性証明 $f(m)$ の生成過程において、属性証明に使用される値 m を、チャレンジMのハッシュ値 $m = h(M)$ に変更した構成となっている。

【0071】従って、本実施形態は、以下に述べる属性証明時のチャレンジに関する動作以外は第1の実施形態と同様の作用効果を有する。すなわち、本実施形態の属性証明時においては、検証者装置Vのチャレンジ生成部33が、チャレンジ m ではなく、チャレンジ $M \in {}_R Z_q^*$ を生成して前述同様に(開示要求する属性群 Λ と共に)利用者装置Aに送信する。

【0072】利用者装置Aの属性証明生成部15は、チャレンジMのハッシュ値 $m = h(M)$ を計算し、このハッシュ値 m に対する属性証明 $f(m)$ を前述同様に計算し、前述同様に(検証用データ(j, a_i, r_i)と共に)検証者装置Vに送信する。

【0073】また、検証者装置Vの属性証明検証部34は、利用者装置Aから属性証明 $f(m)$ を受けると、チャレンジMのハッシュ値 $m = h(M)$ を計算した後、このハッシュ値 m を用いて前述同様に属性証明 $f(m)$ の正当性を検証する。以下、第1の実施形態と同様に動作する。

【0074】上述したように本実施形態によれば、第1の実施形態の効果に加え、チャレンジMのハッシュ値 $m = h(M)$ に対して属性証明 $f(m)$ を行なうことから、セキュリティ性を向上させることができる。

【0075】(第3の実施形態)図4は本発明の第3の実施形態に係る属性証明システムの構成を示す模式図である。本実施形態は、第1及び第2の実施形態の変形例であり、第1及び第2の実施形態と異なる点は、チャレンジMが利用者(証明者)装置Aにより生成される点である。すなわち、本実施形態は、属性証明の一種として、自己の文書(チャレンジ)Mに対する属性署名(属性付き署名)を実現するものである。

【0076】具体的には利用者装置Aの属性証明生成部15が、前述した機能に加え、文書MとしてのチャレンジMを生成し、このチャレンジMのハッシュ値 $m = h$

(M)を算出し、このハッシュ値 m の属性証明(文書Mに対する署名) $f(m)$ を算出し、且つ(検証者装置Vからの開示要求無しに)開示する属性群 Λ を用意し、これらチャレンジM、属性証明 $f(m)$ 、属性群 Λ の検証用データを検証者装置Vに送信可能な構成となっている。

【0077】ここで、文書Mとしては、属性署名の対象となる電子化文書であれば任意の文書が使用可能であり、その種の電子化文書の典型的な例としては、アンケート調査の回答文書などがある。開示する属性としては、前述同様に必要最小限の属性であり、例えば「性別(例、男性)」、「年齢(例、26歳)」、「職業(例、会社員)」等がある。なお、開示する属性は、ここでは利用者装置Aに用意される場合を述べたが、第1及び第2の実施形態と同じく、検証者装置Vから要求されてもよい。

【0078】一方、検証者装置Vでは、属性情報要求部32及びチャレンジ生成部33が省略された構成となる。これに伴い、属性認可書検証部31は、前述した機能において、属性認可書 $Cert_A$ の検証結果の送出先が属性証明検証部34'になっている。

【0079】属性証明検証部34'は、前述した機能に加え、利用者装置Aから受けたチャレンジMを用いてそのハッシュ値 $m = h(M)$ を計算する機能と、得られたハッシュ値 m を用いて前述同様に属性証明 $f(m)$ の正当性を検証する機能をもっている。

【0080】以上のような構成により、属性証明時に、利用者装置Aの属性証明生成部15は、前述した機能に加え、チャレンジMを生成し、そのハッシュ値 $m = h(M)$ を計算し、ハッシュ値 m を用いた属性証明 $f(m)$ を計算する。また、開示する属性群 Λ の検証用情報を用意する。

【0081】しかる後、利用者装置Aの属性証明生成部15は、属性認可書 $Cert_A$ の検証用データ $(v, Cert_A, n, P_A, c_1, \dots, c_n)$ 、チャレンジM、属性証明 $f(m)$ 、開示する属性情報の検証用データ (j, a_i, r_i) を検証者装置Vに送信する。

【0082】検証者装置Vでは、これらを受けると、属性認可書検証部31が、前述した通り、属性認可書 $Cert_A$ の検証用データ $(v, Cert_A, n, P_A, c_1, \dots, c_n)$ に基づいて属性認可書 $Cert_A$ を検証し、検証結果を属性証明検証部34'に送出する。

【0083】属性証明検証部34'は、検証結果が属性認可書 $Cert_A$ の正当性を示すとき、利用者装置Aから受けたチャレンジMを用いてそのハッシュ値 $m = h(M)$ を計算し、このハッシュ値 m を用いて前述同様に属性証明 $f(m)$ の正当性を検証する。以下、第1の実施形態と同様に動作する。

【0084】上述したように本実施形態によれば、第1及び第2の実施形態の効果に加え、さらに、利用者(証明者)が自らチャレンジMを生成して属性署名(属性付

き署名)を行なうことができる。この属性署名は、例えばアンケート調査の回答文書MとしてのチャレンジMなどのハッシュ値 $m = h(M)$ に対して実施できる。

【0085】なお、本実施形態の変形例として、開示する属性が、第1及び第2の実施形態と同じく、検証者装置Vから要求されてもよい。この変形例の場合、属性証明時に、利用者装置Aの属性証明生成部15は、属性証明時に、第1の実施形態と同じく、属性認可書 $Cert_A$ の検証用データ $(v, Cert_A, n, P_A, c_1, \dots, c_n)$ を検証者装置Vに送信し、検証者装置Vの属性認可書検証部31は、前述した通り、属性認可書 $Cert_A$ の検証結果を属性証明検証部34'に送出する。属性証明検証部34'は、検証結果が属性認可書 $Cert_A$ の正当性を示すとき、開示して欲しい属性からなる属性群 Λ を利用者装置Aに送信する。利用者装置Aでは、属性群 Λ を受けると、属性証明生成部15が、チャレンジMを生成し、そのハッシュ値 $m = h(M)$ を計算し、ハッシュ値 m を用いた属性証明 $f(m)$ を計算する。また、開示する属性群 Λ の検証用情報を用意する。といった動作となる。このような変形例としても本発明を同様に実施して同様の効果を得ることができる。

【0086】(第4の実施形態)次に、本発明の第4の実施形態に係る属性証明システムについて説明する。

【0087】本実施形態は、第1～第3の実施形態の変形例であり、生成器 g を利用者装置Aが生成する値とし、属性認可書発行時に、生成器 g を利用者装置Aから属性認可書発行機関装置ACAに提示する方式となっている。

【0088】これに伴い、利用者装置A、属性認可書発行機関装置ACA及び検証者装置Vの構成が以下のように変更される。利用者装置Aにおいては、鍵生成部11が、前述した機能に加え、生成器 g を生成する機能を有する。

【0089】属性情報生成部12は、前述した機能に加え、属性認可書発行機関装置ACAに対し、前述した情報 (P_A, Λ_0) と、生成器 g とを提示する機能を有する。

【0090】属性証明生成部15は、前述した機能に加え、生成器 g を含めて属性情報の検証用データ $(g, v, Cert_A, n, P_A, c_1, \dots, c_n)$ を検証者装置Vに送信する機能をもっている。

【0091】一方、属性認可書発行機関装置ACAにおいては、属性認可書発行部22が、前述した機能に加え、属性認可書発行時に、下記のように、生成器 g を含めた内容の属性認可書 $Cert_A$ を発行する機能をもっている。

【0092】 $Cert_A = \text{Sig}_{CA} [h(g || P_A || n || c_1 || \dots || c_n)]$ また一方、検証者装置Vにおいては、属性認可書検証部31が、前述した機能に加え、下記のように、生成器 g を含めた内容の属性認可書 $Cert_A$ を検証す

る機能をもっている。

【0093】 $Veri_{A,C_A}[h(g||P_A||n||c_1||\dots||c_n), Cert_A] = \text{valid?}$ 以上のような構成としても、第1～第3の実施形態と同様の効果を得ることができる。

【0094】(第5の実施形態) 図5は本発明の第5の実施形態に係る検証者装置の構成を示す模式図である。本実施形態は、第1～第5の実施形態の変形例であり、具体的には検証者装置Vが、属性証明検証部34による検証結果に応じて後段の対象システムを利用可能とする対象実行許可部35を備えている。

【0095】ここで、対象実行許可部35は、属性証明検証部35により検証された属性と所定の判定基準とに基づいて、後段の対象システムの実行可否を判定し、実行可の時に実行を許可する機能をもっている。実行可否の判定基準は、任意であり、例えば属性が「男性」で判定基準が「男性」というように完全一致の場合や、属性が「26歳」で判定基準が「20歳以上」というように範囲指定の場合などが使用可能であり、その他、判定基準を検索条件と考えれば周知の検索技術などが適用可能である。

【0096】対象システムの個数及び内容は任意であるが、例えば、「20歳以上」「独身」「男性」の属性が証明された利用者へのみ閲覧させるホームページ等としてもよい。または、「本人」の属性が証明された利用者へのみ証明書を発行するシステム等がある。あるいは、任意の属性と、「属性認可書 $Cert_A$ の発行(要求)日」の属性とが証明され、且つ「属性認可書 $Cert_A$ の発行(要求)日」が有効期限内である利用者のみ実行可能なシステム等がある。

【0097】すなわち、対象実行許可部35は、任意の属性、当該属性に基づく実行可否の判定基準及び各種の対象システムに適用でき、それら実行可否の判定基準や対象システムの内容には限定がない。

【0098】以上のような構成により、第1～第4の実施形態の効果に加え、後段の対象システムを不正な利用者による利用から保護することができる。

【0099】なお、本実施形態は、対象実行許可部35が実行可否を判定する場合を説明したが、実行可否に加*

$$\text{第1検証式 } f(m) \cdot G \equiv VP_A + mV + \sum_{i=1}^l m_i^{l+1} C_i \pmod{p}$$

第2検証式 $C_i \equiv h(a_i || r_i) \cdot G \pmod{p}$

以上のような構成としても、第1～第5の各実施形態の効果を得ることができ、さらに楕円曲線暗号で実現したことにより、鍵長や署名データ長を低減させることができる。なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク(フロッピー(登録商標)ディスク、ハードディスクなど)、光ディスク(CD-ROM、DVDなど)、光磁気ディスク(MO)、半導体メモリなどの記

*え、対象実行許可部35が、検証された属性に基づいて、利用可能な範囲をも設定する機能を有してもよい。

【0100】例えば、機密事項DB及び周知資料DBを有する社内システムの場合、「正社員」の属性をもつ利用者は、社内システム自体と周知資料DBとを利用可能であるが、必ずしも機密事項DBを利用できず、機密事項DBを利用するには更に「機密事項DBの担当部門」及び/又は「部長」以上の属性を必要とする等のように、検証された属性に基づいて、対象システムの実行可能な範囲を定めてもよい。

【0101】あるいは、対象システムが複数の実行パラメータをもつ場合(例、シミュレーションシステム、ロールプレイングゲームシステム、占いゲームシステム等)、システム全体を実行可能であるが、対象実行許可部35が、検証された属性に基づいて、実行パラメータを設定する機能を備えてもよい。

【0102】(第6の実施形態) 次に、本発明の第6の実施形態に係る属性証明システムについて説明する。本実施形態は、第1～第5の各実施形態の変形例であり、概略的には、第1～第5の各実施形態における離散対数問題を、有限群 $E(GF(p))$ 上の楕円離散対数問題(EDLP)に書換えた構成となっている。

【0103】ここで、有限群 $E(GF(p))$ は、有限体 $GF(p)$ 上の楕円曲線を意味しており、 $a, b \in GF(p)$ を $4a^3 + 27b^2 \neq 0$ なる元とすると、 $\{(x, y) \in GF(p)^2 \mid y^2 = x^3 + ax + b\} \cup O$

と表現される。但し、 O : 仮想的な無限遠点。

【0104】すなわち、本実施形態は、第1～第5の各実施形態を楕円曲線暗号に適用した変形例である。具体的には、第1の実施形態に明記され且つ第2～第5の各実施形態に引用される各式が以下のように書換えられる。なお、 G は楕円曲線上の点とする。

【0105】公開鍵 $P_A = S_A \cdot G \pmod{p}$

($= G + \dots + G : G$ を S_A 回加算)

コミット値 $C_i = b_i \cdot G \pmod{p}$

コミット値 $V = u \cdot G \pmod{p}$

【数3】

憶媒体に格納して頒布することもできる。

【0106】また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【0107】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS(オペレーティングシステム)や、データベース管理ソフト、ネットワークソフト等のMW

(ミドルウェア)等が本実施形態を実現するための各処理の一部を実行しても良い。

【0108】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【0109】また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【0110】尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【0111】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0112】なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。例えば「属性情報」の語は、1個で独立して意味をもつ単位情報

(例、単語、名称や小文書など、完結した情報)に限らず、全部又はしきい値個数以上が統合されると意味をもつ分散情報(例、秘密情報の一部)であってもよい。すなわち、「属性情報」の語は、任意の部分情報であればよく、社会通念上の「属性(その物の有する特徴・性質)」を示す内容ではなくても、本発明の範囲に含まれる。

【0113】例えば、本発明を周知の段階的秘密交換プロトコルの適用対象(例、電子商取引など)に適用し、秘密情報(例、決済情報や契約文書)を所定サイズ毎に属性情報とした場合、社会通念上「決済情報や契約文書の一部」を示す内容であっても、本発明の「属性」に含まれる。

【0114】但し、この場合、利用者装置と検証者装置の機能を併せもつ2台の利用・検証者装置が使用され、互いに選択的な属性情報の開示を繰り返し、最終的には全ての属性情報を開示し合うという構成になる。すなわち、属性情報の選択的な開示は、1回に限らず、複数回繰り返してもよい。また、利用者装置Aと検証者装置Vとは、一方向で固定的な場合に限らず、双方向で交替的な場合も可能である。

【0115】一方、属性情報の定義に伴い、「属性認可書」の語は、各部分情報(各属性情報)の集合に対するデジタル署名であればよく、社会通念上の「属性を認可」したものでなくても本発明の範囲に含まれる。前述の例では、社会通念上の「決済情報や契約文書」が本発明の「属性認可書」に含まれる。

【0116】また、「利用者装置」及び「検証者装置」の語は、上述した機能を有するものであれば、社会通念上の「利用者」「検証者」には限定されない。例えば、本発明を「数字(属性情報)を揃えるスピードくじ」に適用する場合、スピードくじ(属性認可書)の販売者が「利用者装置」を用い、社会通念上の利用者が「検証者装置」を使うことになるが、このような場合も本発明の範囲に含まれる。

【0117】また、各実施形態及び変形例は可能な限り適宜組み合わせる実施してもよく、その場合、組み合わせられた効果が得られる。また、各実施形態及び変形例の組合せに限らず、各装置(利用者装置A、属性認可書発行機関装置ACA、検証者装置V)も、適用されるシステムに応じて適宜組合せて実施できる。

【0118】例えば、第1～第6の実施形態の場合、属性認可書発行機関装置ACAと検証者装置Vとを組合せてもよい。また、前述したスピードくじのシステムの場合等では、利用者装置Aと属性認可書発行機関装置ACAとを組合せてもよい。さらに、前述した段階的秘密交換のシステムの場合等では、利用者装置Aと検証者装置Vとを組合せてもよい。

【0119】さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【0120】その他、本発明はその要旨を逸脱しない範囲で種々に変形して実施できる。

【0121】

【発明の効果】以上説明したように本発明によれば、各種システムに応用でき、情報化社会の発展に寄与できる属性証明プログラム及び装置を提供できる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る属性証明システムの構成を示す模式図

【図2】同実施形態における属性認可書発行の動作を説明するためのフローチャート

【図3】同実施形態における属性証明の動作を説明するためのフローチャート

【図4】本発明の第3の実施形態に係る属性証明システムの構成を示す模式図

【図5】本発明の第5の実施形態に係る検証者装置の構成を示す模式図

【図6】本発明の骨子を説明するための模式図

【図7】本発明の骨子を従来と比較して説明するための模式図

【符号の説明】

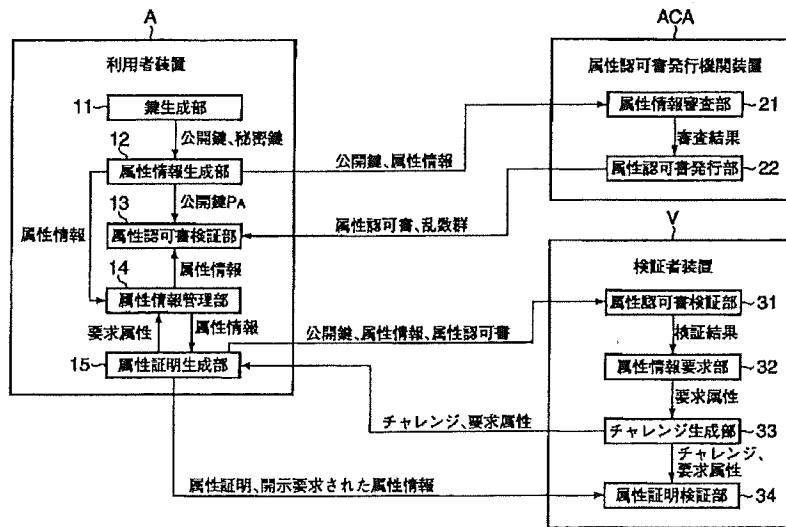
50 A…利用者装置

11…鍵生成部
 12…属性情報生成部
 13…属性認可書検証部
 14…属性情報管理部
 15…属性証明生成部
 ACA…属性認可書発行機関装置
 21…属性情報審査部
 22…属性認可書発行部

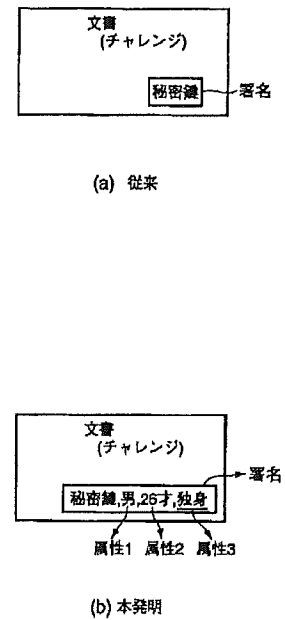
* 22…属性認可書発行部
 V…検証者装置
 31…属性認可書検証部
 32…属性情報要求部
 33…チャレンジ生成部
 34, 34'…属性証明検証部

*

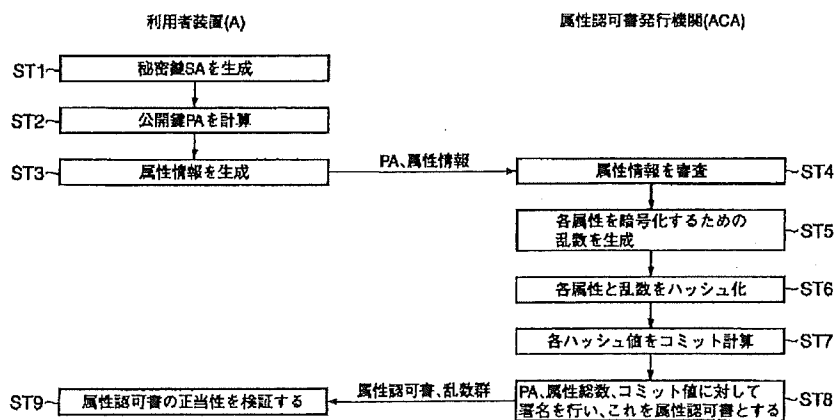
【図1】



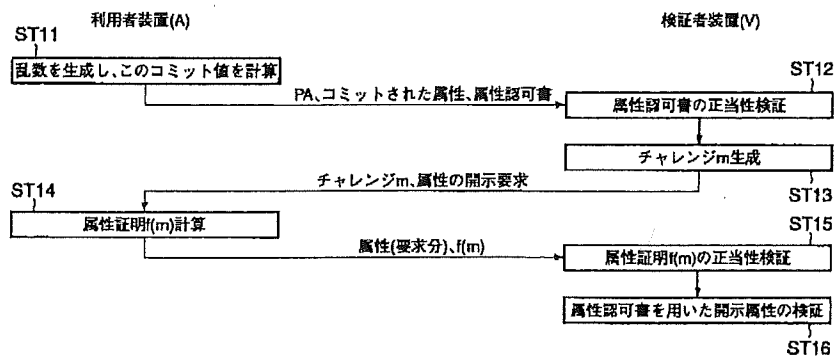
【図7】



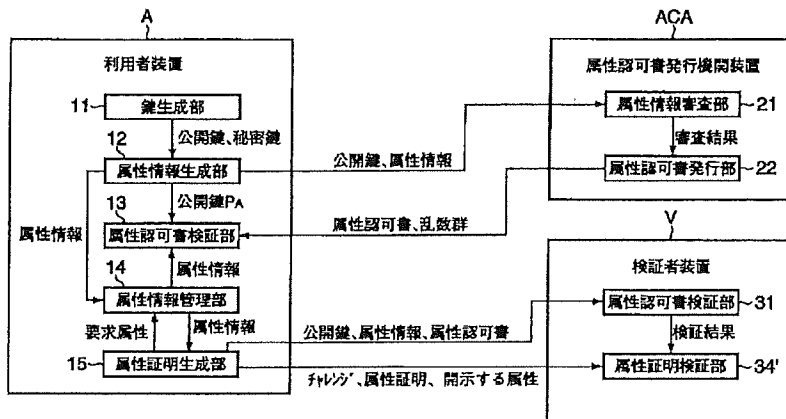
【図2】



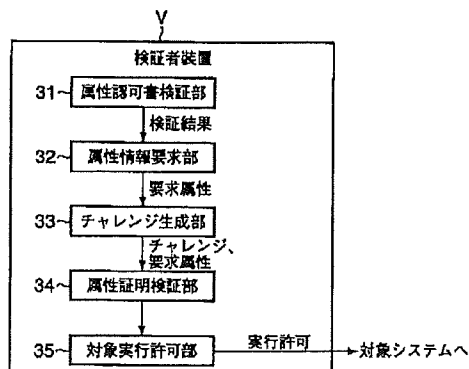
【図3】



【図4】



【図5】



【図6】

